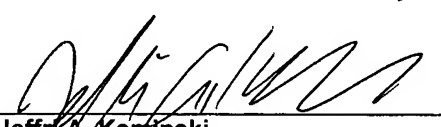




ZZW
AF
\$

TRANSMITTAL OF APPEAL BRIEF			Docket No. 35997-215657
In re Application of: Tatu YLONEN et al.			
Application No. 10/020,299-Conf. #8259	Filing Date December 7, 2001	Examiner Jeffrey D. Popham	Group Art Unit 2137
Invention: APPLICATION GATEWAY SYSTEM, AND METHOD FOR MAINTAINING SECURITY IN A PACKET-SWITCHED INFORMATION NETWORK			
<u>TO THE COMMISSIONER OF PATENTS:</u>			
Transmitted herewith is the Appeal Brief in this application, with respect to the Notice of Appeal filed: <u>August 25, 2006</u>			
The fee for filing this Appeal Brief is <u>\$500.00</u>			
<input checked="" type="checkbox"/> Large Entity <input type="checkbox"/> Small Entity			
<input checked="" type="checkbox"/> A petition for extension of time is also enclosed.			
The fee for the extension of time is <u>\$450.00</u>			
<input type="checkbox"/> A check in the amount of _____ is enclosed.			
<input checked="" type="checkbox"/> Charge the amount of the fee to Deposit Account No. <u>22-0261</u> This sheet is submitted in duplicate.			
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.			
<input checked="" type="checkbox"/> The Director is hereby authorized to charge any additional fees that may be required or credit any overpayment to Deposit Account No. <u>22-0261</u> This sheet is submitted in duplicate.			
 Jeff A. Kaminski Attorney Reg. No. 42,709 VENABLE LLP P.O. Box 34385 Washington, DC 20043-9998 (202) 344-4000		Dated: <u>December 22, 2006</u>	



Docket No.: 35997-215657
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Tatu Ylonen

Art Unit: 2137

Application No: 10/020,299

Examiner: POPHAM, JEFFREY D

Confirmation No: 8259

Filed: December 7, 2001

Atty. Docket No: 35997-215657

Customer No:

For: APPLICATION GATEWAY SYSTEM,
AND METHOD FOR MAINTAINING
SECURITY IN A PACKET-SWITCHED
INFORMATION NETWORK

26694

PATENT TRADEMARK OFFICE

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In furtherance of the Notice of Appeal and a Pre-Appeal Brief Request filed on August 25, 2006, the Appellant submits herewith an Appeal Brief in accordance with 37 C.F.R. § 41.37.

The fees required under § 41.20(b)(2), and any required petition for extension of time for filing this brief and fees therefore, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

12/27/2006 MBERHE 00000021 220261 10020299

01 FC:1402 500.00 DA
02 FC:1252 450.00 DA

I. REAL PARTY IN INTEREST – 37 C.F.R. § 41.37(c)(1)(i)

The real party in interest for this appeal is:

SafeNet, Inc.
Bel Camp, MD

The aforementioned real party is a successor in interest to SSH Communications Security Corporation (a company organized under the laws of Finland), which is the assignee of the present application by virtue of assignment from the inventors, Tero Kivinen and Markus Levlin, recorded 03/28/2002, at Reel 012761, Frame 0462.

II. STATEMENT OF RELATED APPEALS AND INTERFERENCES – 37 C.F.R. §

41.37(c)(1)(ii)

There are no other appeals, interferences or judicial proceedings known to the Appellant, Appellant's legal representatives, or the above-noted inventor/assignor, that will directly affect or will be directly affected by or have bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS – 37 C.F.R. § 41.37(c)(1)(iii)

Pending claims 1-74 were rejected in the Final Office Action dated March 28, 2006. All pending claims 1-74 are hereby appealed.

IV. STATUS OF AMENDMENTS – 37 C.F.R. § 41.37(c)(1)(iv)

Applicant filed a Response After Final Rejection on July 24, 2006 and a Notice of Appeal on August 25, 2006. No claim amendments were made after final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER – 37 C.F.R. § 41.37(c)(1)(v)**A. Features of the Invention**

A method and system for handling data packets at a logical borderline that separate an untrusted packet-switched information network from a protected domain in an efficient and secure manner is provided.

The conventional way of protecting a protected domain against hostile attacks from an insecure external information network is to route all data packets transmitted therebetween through a so-called firewall. A conventional a firewall may utilize a packet processor, which filters packets on the basis of the packet header information depending on a set of filtering rules defined by the network supervisor. Alternatively, a firewall may utilize an application gateway, which monitors the packets on the basis of their compliance with a certain protocol in order to decide whether a certain connection proceeds according to that protocol.

A packet processor is fast, but inefficient in filtering undesired packets. An application gateway, on the other hand, is effective in detecting and filtering undesired packets, but requires a great deal of computational effort which can cause delay in processing the packets. The present application describes a system and method that provides the level of security of an application gateway while avoiding the long delays typically caused by the application gateway. Such is achieved by providing a packet processor as well as an application gateway within a firewall computer, where the packets are first examined by the packet processor, which examines the packets to determine if they are associated with the certain protocol that the protocol-specific application gateway handles and, if so, redirects those packets to the application gateway for processing. As a result, the application gateway only those packets that are associated with its protocol and the packet processor processes all the other packets. Accordingly, the firewall benefits from the security of the application gateway without undue delays in processing unassociated packets.

The packets can be directed from the packet processor to the application gateway in a variety of signaling schemes. One embodiment of the present invention utilizes NATting (Network Address Translations), which is a method generally known in the art. In NATting, the destination

information field of the packet is replaced with the address of the application gateway, so that the packet is redirected to the application gateway. Since the NATted packet received by the application gateway no longer contains the original destination address of the packet, such information is signaled from the packet processor to the application gateway. The application gateway then uses the original destination address along with the packet to process the packet.

Instead of replacing the original destination address with the address of the application gateway, in another embodiment of the present invention, the address of the application gateway is prepended as a separate header to the packet at the packet processor and used to direct the packet to the application gateway. Thereafter, the prepended header is stripped from the packet and the packet is processed at the application gateway.

B. The Independent Claims on Appeal – Claims 1, 39, 41, 43, 47, 51, 53, 62, 64, 66, 68, 69 and 71

The following explanation of the claimed subject matter, with reference to the specification and drawings of the instant application, is by way of example and for explanation only. The invention is not limited to the disclosed embodiments, and certain elements may be found in more than one of the disclosed embodiments.

Claim 1 recites a method for handling digital data packets at a logical borderline 103 (i.e. a firewall device) that separates an untrusted packet-switched information network 101 (e.g. the internet) from a protected domain 102 (i.e. a private packet-switched information network), as depicted in FIG. 1. The logical borderline includes a packet processor 110 and an application gateway 111. Please see FIG. 1 and page 8, lines 1-9. The method of claim 1 comprises the steps of intercepting a packet that is in transit between the untrusted packet-switched information network 101 and the protected domain 102 at the packet processor 110 and examining the packet at the packet processor 110 to determine whether it contains digital data that pertains to a certain protocol. Please see FIG. 2, page 8, lines 20-28, and page 9, line 18 through page 10, line 17. If the packet does not contain digital data that pertain to the certain protocol, the packet processor 110 processes the packet. *Id.* However, if the packet contains digital data that pertain to the certain protocol, the packet is redirected to an application gateway part 111 and processed there according to a set of

processing rules based on obedience to the certain protocol. Id. Claim 1 also recites a limitation that the packet processor 110 is a kernel mode process running in a computer device and the application gateway 111 is a user mode process running in a computer device. Please see page 8, line 34 to page 9, line 14.

Claim 39 recites features similar to claim 1, except that it recites in more detail the process of redirecting the packet from the packet processor 110 to the application gateway 111 according to one embodiment of the present invention. As recited in claim 39, if the packet contains digital data that pertain to a certain protocol, the original value of a certain destination information field within the packet is replaced with a replacement value that identifies an application gateway part as the destination of the packet, and redirecting the packet to the application gateway part 111. Please see page 6, lines 21-27. The packet processor 110 then indicates to the application gateway 111 the original value of the destination information field found in the packet at the moment of intercepting the packet at the packet processor part. Finally, the indicated original value of the destination information field is used at the application gateway 111 in processing the packet according to a set of processing rules based on obedience to its certain protocol. Please see page 6, line 29 – page 7, line 1 and page 14, line 29 – page 15, line 2. Also, unlike claim 1, claim 39 does not recite the packet processor 110 being a kernel mode process and the application gateway 111 being a user mode process.

Claim 41 also recites features similar to claim 1, except that it recites the process of redirecting the packet from the packet processor 110 to the application gateway 111 according to the second embodiment of the present invention. As recited in claim 41, if the packet contains digital data that pertain to a certain protocol, a header is prepended to the packet at the packet processor 110, the prepended header containing a value that identifies an application gateway 111 as the destination of the packet, and the packet is redirected to the application gateway 111. Please see page 17, lines 10-16. The prepended header is then stripped from the packet at the application gateway 111 and the original value of the destination information field in the packet is used at the application gateway 111 in processing the packet according to a set of processing rules based on obedience to its certain protocol. Please see page 17, lines 16-21. Also, similar to claim 39, claim

41 does not recite the packet processor 110 being a kernel mode process and the application gateway 111 being a user mode process.

Claim 43 and 47 includes limitations similar to claim 39 and 41, respectively, but recite “a method for handling digital data packet at a *packet processing entity* located at a logical borderline ...” (emphasis added). Similarly, claim 51 includes limitations similar to claim 39, but recites “a method for handling digital data packet at an *application gateway entity* located at a logical borderline ...” (emphasis added). Claims 53, 62, 64, 66, 68, 69 and 71 variously include features similar to claims 1, 39 or 41, recited in form of a system, device, or software program.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL – 37 C.F.R. § 41.37(c)(1)(vi)

A. Whether the Examiner has established that claim 1-3, 7, 8, 12, 14, 19-31, 33-40, 43-46, 49-55, 58-63, 66-70, 73 and 74 is unpatentable under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Number 6,754,706 to Gbadegesin (hereinafter “Gbadegesin”).

B. Whether the Examiner has established that claims 4, 15-17, 41, 42, 47, 48, 56, 57, 64, 65, 71, and 72 are unpatentable under 35 U.S.C. § 103(a) over Gbadegesin in view of U.S. Patent Application Publication No. 2002/0124090 to Poier (hereinafter “Poier”).

C. Whether the Examiner has established that claims 5 and 6 are unpatentable under 35 U.S.C. § 103(a) over Gbadegesin in view of Poier, in further view of the article The TCP Datagram, I wanted to know and now you can too (hereinafter “Datagram”).

D. Whether the Examiner has established that claims 9, 10, and 32 are unpatentable under 35 U.S.C. § 103(a) over Gbadegesin in view of the article 3.3 Connectionless Transport: UDP (hereinafter “UDP”).

E. Whether the Examiner has established that claims 11 and 13 are unpatentable under 35 U.S.C. § 103(a) over Gbadegesin in view of the article WTCP: an Efficient Transmission Control Protocol for Wired/Wireless Internetworking to Cheng (hereinafter “Cheng”).

F. Whether the Examiner has established that claims 18 is unpatentable under 35 U.S.C. § 103(a) over Gbadegesin in view of Poier, in further view of the article RFC 1928 – SOCKS Protocol Version 5 to Leech (hereinafter “Leech”).

VII. ARGUMENT – 37 C.F.R. §41.37(c)(1)(vii)**A. The Rejection of Claims 1-3, 7, 8, 12, 14, 19-31, 33-40, 43-46, 49-55, 58-63, 66-70, 73 and 74 Under 35 U.S.C. § 102(e)**

On pages 4-20 of the Final Office Action, claim 1-3, 7, 8, 12, 14, 19-31, 33-40, 43-46, 49-55, 58-63, 66-70, 73 and 74 are rejected under 35 U.S.C. § 102(e) as being anticipated by Gbadegesin. The Appellant respectfully traverses these rejections and hereby appeals the same.

A claim is anticipated “only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.” *MPEP 2131* citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987). Further, “[t]he identical invention must be shown in as complete detail as is contained in the ... claim.” *MPEP § 2131.02* citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Finally, even within a single reference, separate portions of that reference cannot be properly combined in the absence of “particular findings...as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected [those portions] for combination in the manner claimed.” *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000).

One fundamental difference between the claimed invention and the cited art is that the claimed invention examines the packet to determine if the data in the packet pertains to a certain protocol. See claim 1, for example, “examining the packet at the packet processor part in order to determine, whether the packet contains digital data that pertains to a certain protocol,”. None of the cited art disclose or suggest determining if data in the packet pertains to a certain protocol.

It is asserted that observing the packet is the same as determining in the data in the packet pertains to a certain protocol Please see Advisory Action of August 14, 2006. Even if Gbadegesin observes the packet and redirects the packet based on that observation, this is not the same as examining the data within the packet. Using an analogy, the packet is a box and the contents of the box are the data within the packet. The box can be examined to determined if the box has certain characteristics. For example the box can be observed to determine if it has a certain color, is sealed in a particular manner, includes an address label, etc. However, observing the box (packet) provides no information on the contents of the box (data in the packet). Without examining the contents of

the box (data in the packet), there is no way to determine if the contents (data) has certain characteristics. The present claims recite determining if the data in the packet pertain to a certain protocol. Gbadegesin describes examining the packet itself. These are fundamentally different things.

More specifically, Gbadegesin relates to network address translation (NAT) and proxy applications used to allow a computer C1, having a private IP address 62 on a private network 60, to communicate with a public network, such as the internet 64. Gbadegesin points out that a conventional NAT machine, which changes the source address 70 of the message packets from the private address of the client computer to its public IP address, its translation of source addresses is fixed within its programming and it does not allow any application control of the address translation that is performed. *See Col. 1: 35-43 and Col. 2: 1-10*. In traditional proxies, on the other hand, the interface is provided in user mode so that the proxy 98 is addressed directly by the client machine and proxy 98 then decides whether and to whom to forward the communication on the public network. Proxies, however, require that the client applications be set up to operate with a proxy 98, which many applications are unable to do. *See Col. 2: 18-40*. Transparent proxies attempt to improve on traditional proxies by implementing a NAT 95 to redirect all addresses to its proxy application 97, thereby utilizing the value of traditional proxies without the need for client to address the proxy directly. *See Col. 2: 51-65 and Col. : 2-6*. However, the redirection is fixed within the NAT 95, thereby requiring all communication to be transferred up to the proxy at the user-level and back down to the kernel level prior to being transmitted to the server, which creates long delays in transmission. *See Col. 3: 9-14*.

Accordingly, Gbadegesin discloses an intelligent transparent proxy that combines a NAT and a proxy application to provide the benefits of both a proxy server and a NAT while minimizing the transmission delays of traditional and proxies. *See Col. 3: 35-49*. In Gbadegesin, a generalized network address translator (gNAT) module 106 examines a packet to determine if it is from a recognized or new and unrecognized session. The packets in new and unrecognized sessions are forwarded by the gNAT module 106 to the packets to proxy 104 for processing. *See FIG. 10 and Col. 7: 66 to Col. 8: 30 and Col. 9: 66 to Col. 10: 36*. The packets that relate to a recognized session, on the other hand, are not redirected to the proxy 104; instead, these packets are handled by

the gNAT module 106, which translates these packets' addresses according to a mapping 118. *See FIG. 10 and Col. 10: 18-23.*

In summary, the module 106 in Gbadegesin determines whether a packet relates to a ***recognized or unrecognized session***. If a packet relates to an unrecognized session, the packet is forwarded to proxy 104. If the packet relates to recognized session, the module 106 translates the address according to a dynamic mapping 118 and forwards the packet accordingly. Gbadegesin contains no teaching or suggestion of any function that determines whether the packet contains digital data that pertains to a certain protocol and redirecting the packet based on that determination. None of gNAT module 106 or proxy 104 in Gbadegesin, which the Examiner has respectively construed as equivalents to the packet processor part and the application gateway part of the present invention, makes any determination of the protocol of the data in the packet or bases any decision upon such a determination.

In comparison, the independent claims of the present application recite that the packet processor part ***determines whether the packet contains digital data that pertains to a certain protocol***. Packets that include data that pertain to the certain protocol are redirected to an application gateway part for processing according to a set of processing rules based on obedience to that certain protocol. Those packets that do not contain digital data that pertains to the certain protocol are processed by the packet processor part. This is entirely different from the system in Gbadegesin which the kernel mode translation module forwards data based on whether the data belongs to an unrecognized session or a recognized session.

In the Advisory Action dated August 14, 2006, the Examiner argues that Gbadegesin teaches determining whether a packet contain digital data that pertains to a certain protocol in Col. 8: 16 to Col. 9: 5, where it discusses a 'port-redirect command', according to which packets are forwarded to the proxy 104. The Examiner argues that this command is equivalent to the 'certain protocol' of the present claim. It is respectfully submitted that the Examiner has misconstrued not only the purpose of the port-redirect command, but also the module of Gbadegesin that performs the redirecting according to this command.

In Gbadegesin, the transparent proxy 104 invokes a transparent proxy API 108 to create and issue a ‘dynamic port-redirect’ for TCP port 80, which is the HTTP port. Thereafter, all sessions destined for TCP port 80 are directed instead to the transparent proxy 104. *See Col. 8: 24-49.* Therefore, ‘port-redirect’ command is not a protocol that the digital data of packets have to satisfy; instead, the destination of packets (i.e. TCP port 80) determines whether the packet is directed to proxy 104. Therefore, the ‘certain protocol’, as recited in claim 1, is not taught or suggested by Gbadegesin. Furthermore, in Gbadegesin, the **network gateway**, and not the gNTP module 106, determines that the client’s connection request matches the transparent proxy’s commanded redirect. Therefore, the packet processor part of the present claim, which makes the determination of redirecting packets to the application gateway, is not suggested or taught by Gbadegesin.

Additionally, Gbadegesin does not disclose determining if the data in the packet conforms to a certain protocol (HTTP). The data in the packet is not examined at all. Even if Gbadegesin observes the packet and redirects the packet based on that observation, this is not the same as examining the data within the packet. Referring again to the above analogy, the packet is a box and the contents of the box are the data within the packet. The box can be examined to determine if the box has certain characteristics. For example the box can be observed to determine if it has a certain color, is sealed in a particular manner, includes an address label, etc. However, observing the box (packet) provides no information on the contents of the box (data in the packet). Without examining the contents of the box (data in the packet), there is no way to determine if the contents (data) has certain characteristics. The present claims recite determining if the data in the packet pertain to a certain protocol. Gbadegesin describes examining the packet. These are fundamentally different things.

The Appellant respectfully submits that Gbadegesin does not disclose, teach or suggest each and every element of independent claims 1, 39, 43, 51, 53, 62, 66, 68, and 69. For example, claim 1 recites a “method for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain,” that comprises “examining the packet at the packet processor part in order to determine, whether the packet contains digital data that pertains to a certain protocol,” and “if the packet is found to contain digital data that pertains to said certain protocol, redirecting the packet to an application gateway part and processing the packet

at the application gateway part according to a set of processing rules based on obedience to said certain protocol”. It is respectfully submitted that none of these features are taught or suggested by Gbadegesin.

B. Claims 4, 15-17, 41, 42, 47, 48, 56, 57, 64, 65, 71, and 72 under 35 U.S.C. § 103(a) are rejected as being unpatentable over Gbadegesin in view of U.S. Patent Application Publication No. 2002/0124090 to Poier (hereinafter “Poier”).

(1) Claims 4 and 15-17 depend from claim 1. Poier does not supplement Gbadegesin to teach or suggest the features missing from Gbadegesin. Claim 1 is in condition for allowance, as discussed above. Thus, claims 4 and 15-17 are also in condition for allowance because of their dependence on an allowable claim.

(2) Claim 41 recites “A method for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising the steps of: intercepting, at a packet processor part, a packet that is in transit between the untrusted packet-switched information network and the protected domain, examining the packet at the packet processor part in order to determine, whether the packet contains digital data that pertains to a certain protocol, if the packet is not found to contain digital data that would pertain to said certain protocol, processing the packet at the packet processor part, and if the packet is found to contain digital data that pertains to said certain protocol, prepending a header to the packet at the packet processor part, the prepended header containing a value that identifies an application gateway part as the destination of the packet, and redirecting the packet to the application gateway part, stripping the prepended header from the packet at the application gateway part and using the original value of the destination information field in the packet at the application gateway part in processing the packet according to a set of processing rules based on obedience to said certain protocol.”

The Action relies on Poier for a teaching of prepending a header. However, Poier does not teach the above identified claim elements which are also not taught by Gbadegesin. For reasons similar to those given in support of claim 1, claim 41 is in condition for allowance.

Claim 42, which depends from claim 41, is also in condition for allowance due to its dependence on an allowable claim.

(3) Claim 47 is allowable for reasons analogous to those given in support of claim 41.

Claim 48, which depends from claim 47, is also in condition for allowance due to its dependence on an allowable claim.

(4) Claims 56 and 57 depend from claim 53. Claim 53 is in condition for allowance, as discussed above. Thus, claims 56 and 57 are also in condition for allowance because of their dependence on an allowable claim.

(5) The Action rejects claim 64. Claim 64 is allowable for reasons analogous to those given in support of claim 41.

Claim 65, which depends from claim 64, is also in condition for allowance due to its dependence on an allowable claim.

(6) The Action rejects claim 71. Claim 71 is allowable for reasons analogous to those given in support of claim 41.

Claim 72, which depends from claim 71, is also in condition for allowance due to its dependence on an allowable claim.

C. Claims 5 and 6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gbadegesin in view of Poier, in further view of the article The TCP Datagram, I wanted to know and now you can too (hereinafter “Datagram”).

Claims 5 and 6 depend from claim 1. Datagram does not supplement Gbadegesin to teach or suggest the features missing from Gbadegesin. Claim 1 is in condition for allowance, as discussed above. Thus, claims 5 and 6 are also in condition for allowance because of their dependence on an allowable claim.

D. Claims 9, 10, and 32 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gbadegesin in view of the article 3.3 Connectionless Transport: UDP (hereinafter “UDP”).

Claims 9, 10, and 32 depend from claim 1. UDP does not supplement Gbadegesin to teach or suggest the features missing from Gbadegesin. Claim 1 is in condition for allowance, as

discussed above. Thus, claims 9, 10, and 32 are also in condition for allowance because of their dependence on an allowable claim.

E. Claims 11 and 13 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Gbadegesin in view of the article WTCP: an Efficient Transmission Control Protocol for Wired/Wireless Internetworking to Cheng (hereinafter “Cheng”).

Claims 11 and 13 depend from claim 1. Cheng does not supplement Gbadegesin to teach or suggest the features missing from Gbadegesin. Claim 1 is in condition for allowance, as discussed above. Thus, claims 11 and 13 are also in condition for allowance because of their dependence on an allowable claim.

F. Claim 18 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Gbadegesin in view of Poier, in further view of the article RFC 1928 – SOCKS Protocol Version 5 to Leech (hereinafter “Leech”).

Claim 18 depends from claim 1. Leech does not supplement Gbadegesin to teach or suggest the features missing from Gbadegesin. Claim 1 is in condition for allowance, as discussed above. Thus, claim 18 is also in condition for allowance because of its dependence on an allowable claim.

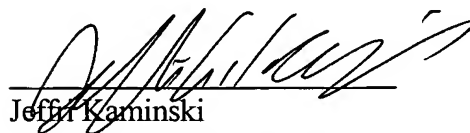
VIII. CONCLUSION

In view of the foregoing arguments, the Applicant respectfully requests reversal of the Examiner's rejections of all claims.

Respectfully submitted,

Date:

12/22/06



Jeff Kaminski

Registration No. 42,709

VENABLE LLP

P.O. Box 34385

Washington, D.C. 20043-9998

Telephone: (202) 344-4000

Fax: (202) 344-8300

DC2-813447

IX. CLAIMS APPENDIX - 37 C.F.R. § 41.37(c)(1)(viii)

Appealed Claims:

1. A method for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising the steps of:

- intercepting, at a packet processor part, a packet that is in transit between the untrusted packet-switched information network and the protected domain,
 - examining the packet at the packet processor part in order to determine, whether the packet contains digital data that pertains to a certain protocol,
 - if the packet is not found to contain digital data that would pertain to said certain protocol, processing the packet at the packet processor part, and
 - if the packet is found to contain digital data that pertains to said certain protocol, redirecting the packet to an application gateway part and processing the packet at the application gateway part according to a set of processing rules based on obedience to said certain protocol;
- wherein the packet processor part is a kernel mode process running in a computer device and the application gateway part is a user mode process running in a computer device.

2. A method according to claim 1, comprising the steps of:

- regarding a packet that is redirected from the packet processor part to the application gateway part:
 - replacing an original value of a certain destination information field within the packet with a replacement value that identifies the application gateway part as the destination of the packet,
 - indicating from the packet processor part to the application gateway part the original value of the destination information field found in the packet at the moment of intercepting the packet at the packet processor part and
 - using the indicated original value of the destination information field at the application gateway part in processing the packet.

3. A method according to claim 2, comprising additionally the steps of:

- replacing an original value of a certain source information field within the packet with a replacement value that identifies the packet processor part as the source of the packet,
- indicating from the packet processor part to the application gateway part the original value of the source information field found in the packet at the moment of intercepting the packet at the packet processor part and
- using the indicated original value of the source information field at the application gateway part in processing the packet.

4. A method according to claim 2 or 3, wherein steps of indicating the original values of certain fields comprise transmitting the original values of such fields from the packet processor part to the application gateway part together with the redirected packet, said certain fields including at least one of a source field and a destination field.

5. A method according to claim 4, comprising the steps of:

- at the packet processor part:
 - setting the value of a certain bit in the packet to indicate the presence of urgent information within the packet,
 - inserting into a pointer field in the packet a pointer value that points at the end of urgent information within the packet, and
 - inserting the original values of said certain fields as urgent information into the packet immediately before the location pointed at by the pointer value; and
- at the application gateway part:
 - reading the original values of said certain fields from the location in the packet pointed at by the pointer value.

6. A method according to claim 4, comprising the steps of:

- at the packet processor part:
 - setting the value of an options field in the packet to indicate the presence of optional information within the packet, and
 - inserting the original values of said certain fields into the packet as optional information; and
- at the application gateway part:
 - reading the original values of said certain fields from the packet as optional information.

7. A method according to claim 2 or 3, wherein steps of indicating the original values of certain fields comprise transmitting the original values of such fields from the packet processor part to the application gateway part separately from the redirected packet, said certain fields including at least one of a source field and a destination field.

8. A method according to claim 7, comprising the steps of:

- at the packet processor part:
 - composing a messaging packet that conforms to a messaging protocol, and inserting the original values of said certain fields into the messaging packet together with the replacement values, and
 - transmitting the messaging packet to the application gateway part; and
- at the application gateway part:
 - receiving the messaging packet, and
 - associating the original values of said certain fields read from the messaging packet with the replacement values found in the redirected packet.

9. A method according to claim 8, wherein the messaging packet is a User Datagram Protocol packet.

10. A method according to claim 8, wherein the step of transmitting the messaging packet to the application gateway part is performed more than once in order to transmit several redundant copies of the messaging packet to the application gateway part.

11. A method according to claim 7, wherein the packet processor part transmits the original values of said certain fields from the packet processor part to the application gateway part spontaneously.

12. A method according to claim 7, comprising the step of transmitting from the application gateway part to the packet processor part a query for the original values of certain fields, so that the packet processor part only transmits the original values of said certain fields to the application gateway part as a response to said query.

13. A method according to claim 7, wherein the packet processor part transmits the original values of said certain fields from the packet processor part to the application gateway part spontaneously, and if the application gateway part has not received such spontaneously transmitted original values within a certain time limit after the reception of a packet for which such original values would be needed, the application gateway part transmits to the packet processor part a query for the original values of said certain fields, so that the packet processor part also transmits the original values of said certain fields to the application gateway part as a response to said query.

14. A method according to claim 7, comprising the step of transmitting the original values of said certain fields from the packet processor part to an application gateway part running in the same computer device with the packet processor part through a communications routine that is internal to that computer device and relies on functions defined in an operating system of that computer device.

15. A method according to claim 1, comprising the steps of:

- regarding a packet that is redirected from the packet processor part to the application gateway part:

- prepending a header to the packet at the packet processor part, the prepended header containing a value that identifies the application gateway part as the destination of the packet,
- stripping the prepended header from the packet at the application gateway part and
- using the original value of a destination information field in the packet at the application gateway part in processing the packet.

16. A method according to claim 15, wherein the prepended header also contains a value that identifies the packet processor part as the source of the packet.

17. A method according to claim 1, comprising the steps of:

- at the packet processor part:
 - enveloping an original packet to be redirected from the packet processor part to the application gateway part into an enveloping packet; and
- at the application gateway part:
 - extracting the original packet from the enveloping packet.

18. A method according to claim 17, wherein the enveloping packet is a packet according to the Socks protocol.

19. A method according to claim 1, wherein the step of redirecting the packet to an application gateway part involves only transferring the packet to a logically separate entity within the same physical device where the packet processor part resides.

20. A method according to claim 1, wherein the step of redirecting the packet to an application gateway part involves transferring the packet to a device that is physically separate from the device where the packet processor part resides.

21. A method according to claim 1, comprising, after the step of processing the packet at the application gateway part, the further steps of:

- returning the processed packet from the application gateway part to the packet processor part and
- forwarding such a returned packet from the packet processor part towards an original destination that the packet had at the moment of it becoming intercepted.

22. A method according to claim 21, comprising the steps of:

- composing at the packet processor part a mapping function that associates a packet redirected to the application gateway part with an original value of a certain destination information field that said packet had at the moment of it becoming intercepted and
- as a response to receiving a processed packet from the application gateway part to the packet processor part, using said mapping function to restore the original value of the destination information field in that processed packet.

23. A method according to claim 22, wherein the mapping function also associates a packet redirected to the application gateway part with an original value of a certain source information field that said packet had at the moment of it becoming intercepted, and as a response to receiving a processed packet from the application gateway part to the packet processor part, said mapping function is also used to restore the original value of the source information field in that processed packet.

24. A method according to claim 21, comprising the steps of:

- transmitting from the application gateway part to the packet processor part information that associates a processed packet returned from the application gateway part to the packet processor part with an original value of a certain destination information field that said processed packet had at the moment of it becoming intercepted and
- as a response to receiving a processed packet from the application gateway part to the packet processor part, using said transmitted information to restore the original value of the destination information field in that processed packet.

25. A method according to claim 24, comprising the steps of:

- transmitting from the application gateway part to the packet processor part information that associates a processed packet returned from the application gateway part to the packet processor part with an original value of a certain source information field that said processed packet had at the moment of it becoming intercepted and
- as a response to receiving a processed packet from the application gateway part to the packet processor part, using said transmitted information to restore the original value of the source information field in that processed packet.

26. A method according to claim 1, comprising, after the step of processing the packet at the application gateway part, the further step of:

- forwarding such a processed packet from the application gateway part towards an original destination that the packet had at the moment of it becoming intercepted, without circulating the forwarded packet through the packet processor part.

27. A method according to claim 26, comprising the steps of:

- transmitting from the packet processor part to the application gateway part information that associates each packet redirected from the packet processor part to the application gateway part with an original value of a certain destination information field that the redirected packet had at the moment of it becoming intercepted and
- after a packet has been processed at the application gateway part, using said transmitted information to restore the original value of the destination information field in that packet.

28. A method according to claim 27, comprising the steps of:

- transmitting from the packet processor part to the application gateway part information that associates each packet redirected from the packet processor part to the application gateway part with an original value of a certain source information field that the redirected packet had at the moment of it becoming intercepted and

- after a packet has been processed at the application gateway part, using said transmitted information to restore the original value of the source information field in that packet.

29. A method according to claim 1, wherein packets are handled in packet streams, all packets of an individual packet stream having the same values in certain source and destination information fields of each packet, and wherein if the first intercepted packet of a certain packet stream is found to contain digital data that pertains to said certain protocol, that packet and all subsequent packets belonging to the same packet stream are redirected to the application gateway part and processed at the application gateway part according to the set of processing rules based on obedience to said certain protocol.

30. A method according to claim 29, comprising the steps of:

- within the first packet and all subsequent packets of a certain packet stream that is found to contain digital data that pertains to said certain protocol, replacing an original value of a certain destination information field with a replacement value that identifies the application gateway part as the destination of the packets, thus enabling redirecting to the application gateway part,
- indicating from the packet processor part to the application gateway part the original value of the destination information field found in the first redirected packet of a packet stream at the moment of intercepting the packet at the packet processor part and
- using the indicated original value of the destination information field at the application gateway part in processing the packets of the redirected packet stream.

31. A method according to claim 30, comprising the steps of:

- within the first packet and all subsequent packets of a certain packet stream that is found to contain digital data that pertains to said certain protocol, replacing also an original value of a certain source information field with a replacement value that identifies the packet processor part as the source of the packets,

- indicating from the packet processor part to the application gateway part the original value of the source information field found in the first redirected packet of a packet stream at the moment of intercepting the packet at the packet processor part and
- using the indicated original value of the source information field at the application gateway part in processing the packets of the redirected packet stream.

32. A method according to claim 30 or 31, wherein the step of indicating from the packet processor part to the application gateway part the original values of certain information fields comprises at least one repetition in order to transmit redundant indications from the packet processor part to the application gateway part.

33. A method according to claim 29, wherein the packets of an individual packet stream belong to an individual TCP connection.

34. (Previously presented) A method according to claim 1, comprising, between the steps of redirecting the packet to the application gateway part and processing the packet at the application gateway part, a step of removing from the redirected packet any traces of it having been redirected, so that the application gateway part processes the packet as if it had received the packet for processing immediately after the packet was intercepted.

35. A method according to claim 34, comprising, after the step of processing the packet at the application gateway part, the steps of:

- re-inserting into the processed packet the redirection information that was removed from the packet before processing the packet at the application gateway part, so that after the re-inserting the packet contains values that identify the application gateway part as the source and the packet processor part as the destination of the packet,
- returning the processed packet from the application gateway part to the packet processor part and

- forwarding such a returned packet from the packet processor part towards an original destination that the packet had at the moment of it becoming intercepted.

36. A method according to claim 1, comprising the step of:

- after a certain packet has been redirected from the packet processor part to the application gateway part, dynamically establishing a new instruction for the packet processor part regarding the redirecting of subsequently arriving packets that have a certain relationship to the packet that was redirected from the packet processor part to the application gateway part.

37. A method according to claim 36, comprising the steps of:

- detecting at the application gateway part that a packet that was redirected from the packet processor part to the application gateway part contains data that pertains to a certain control channel defined in a protocol that also defines a data channel associated with said control channel,
- establishing a new instruction for the packet processor part to redirect to the application gateway part subsequently arriving packets that contain data that pertains to said data channel, and
- communicating the established new instruction from the application gateway part to the packet processor part.

38. A method according to claim 36, comprising the steps of:

- detecting that a packet that was redirected from the packet processor part to the application gateway part is associated with a certain first port number and contains data that pertains to a certain protocol that defines that also a certain second port number should be reserved to said certain protocol, and
- establishing a new instruction for the packet processor part to redirect to the application gateway part subsequently arriving packets that are associated with said second port number.

39. A method for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising the steps of:

- intercepting, at a packet processor part, a packet that is in transit between the untrusted packet-switched information network and the protected domain,
- examining the packet at the packet processor part in order to determine, whether the packet contains digital data that pertains to a certain protocol,
- if the packet is not found to contain digital data that would pertain to said certain protocol, processing the packet at the packet processor part, and
- if the packet is found to contain digital data that pertains to said certain protocol,
 - replacing an original value of a certain destination information field within the packet with a replacement value that identifies an application gateway part as the destination of the packet, and redirecting the packet to the application gateway part,
 - indicating from the packet processor part to the application gateway part the original value of the destination information field found in the packet at the moment of intercepting the packet at the packet processor part and
 - using the indicated original value the destination information field at the application gateway part in processing the packet according to a set of processing rules based on obedience to said certain protocol.

40. A method according to claim 39, additionally comprising the steps of:

- if the packet is found to contain digital data that pertains to said certain protocol, replacing also an original value of a certain source information field within the packet with a replacement value that identifies the packet processing part as the destination of the packet before redirecting the packet to the application gateway part,
- indicating from the packet processor part to the application gateway part the original value of the source information field found in the packet at the moment of intercepting the packet at the packet processor part and
- using the indicated original value the source information field at the application gateway part in processing the packet according to a set of processing rules based on obedience to said certain protocol.

41. A method for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising the steps of:

- intercepting, at a packet processor part, a packet that is in transit between the untrusted packet-switched information network and the protected domain,
- examining the packet at the packet processor part in order to determine, whether the packet contains digital data that pertains to a certain protocol,
- if the packet is not found to contain digital data that would pertain to said certain protocol, processing the packet at the packet processor part, and
- if the packet is found to contain digital data that pertains to said certain protocol,
 - prepending a header to the packet at the packet processor part, the prepended header containing a value that identifies an application gateway part as the destination of the packet, and redirecting the packet to the application gateway part,
 - stripping the prepended header from the packet at the application gateway part and
 - using the original value of the destination information field in the packet at the application gateway part in processing the packet according to a set of processing rules based on obedience to said certain protocol.

42. A method according to claim 41, additionally comprising the steps of:

- if the packet is found to contain digital data that pertains to said certain protocol, inserting into the prepended header also a value that identifies the packet processor part as the source of the packet before redirecting the packet to the application gateway part, and
- using the original value of the source information field in the packet at the application gateway part in processing the packet according to a set of processing rules based on obedience to said certain protocol.

43. A method for handling digital data packets at a packet processing entity located at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising the steps of:

- intercepting a packet when the packet is in transit between the untrusted packet-switched information network and the protected domain,
- examining the packet in order to determine, whether the packet contains digital data that pertains to a certain protocol,
- if the packet is not found to contain digital data that would pertain to said certain protocol, processing the packet at the packet processing entity, and
- if the packet is found to contain digital data that pertains to said certain protocol,
 - replacing an original value of a certain destination information field within the packet with a replacement value that identifies an application gateway part as the destination of the packet,
 - redirecting the packet to the application gateway part for processing according to a set of processing rules based on obedience to said certain protocol, and
 - indicating to the application gateway part the original value of the destination information field found in the packet at the moment of intercepting the packet at the packet filtering entity.

44. A method according to claim 43, additionally comprising the steps of:

- if the packet is found to contain digital data that pertains to said certain protocol, replacing an original value of a certain source information field within the packet with a replacement value that identifies the packet processing entity as the source of the packet before redirecting the packet to the application gateway part, and
- indicating to the application gateway part also the original value of the source information field found in the packet at the moment of intercepting the packet at the packet processing entity.

45. A method according to claim 43, additionally comprising the steps of:

- receiving a packet from the application gateway part after processing according to a set of processing rules based on obedience to said certain protocol,

- restoring the destination information field within the packet to contain the original value that was previously replaced with a replacement value that identified the application gateway part as the destination of the packet, and
- releasing the packet towards a destination that is identified by the original value.

46. A method according to claim 45, additionally comprising the step of restoring a source information field within the packet that was received from the application gateway part to contain an original value that was previously replaced with a replacement value that identified the packet processor part as the source of the packet.

47. A method for handling digital data packets at a packet processing entity located at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising the steps of:

- intercepting a packet when the packet is in transit between the untrusted packet-switched information network and the protected domain,
- examining the packet in order to determine, whether the packet contains digital data that pertains to a certain protocol,
- if the packet is not found to contain digital data that would pertain to said certain protocol, processing the packet at the packet processing entity, and
- if the packet is found to contain digital data that pertains to said certain protocol,
 - prepending a header to the packet, the prepended header containing a value that identifies an application gateway part as the destination of the packet, and
 - redirecting the packet to the application gateway part for processing according to a set of processing rules based on obedience to said certain protocol.

48. A method according to claim 47, additionally comprising the step of:

- if the packet is found to contain digital data that pertains to said certain protocol, inserting into the prepended header also a value that identifies the packet processing entity as the source of the packet before redirecting the packet to the application gateway

part.

49. A method according to any of claims 1, 39, 41, 43 or 47, wherein the step of examining the packet in order to determine, whether the packet contains digital data that pertains to a certain protocol, involves handling the packet according to a set of packet filtering rules.

50. A method according to any of claims 1, 39, 41, 43 or 47, wherein the step of examining the packet in order to determine, whether the packet contains digital data that pertains to a certain protocol, involves checking, whether the packet belongs to a connection or flow all packets of which should be redirected to the application gateway part.

51. A method for handling digital data packets at an application gateway entity located at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising the steps of:

- receiving an intercepted and redirected packet from a packet processor part that intercepts packets when they are in transit between the untrusted packet-switched information network and the protected domain,
- receiving from the packet processor part an original value of a certain destination information field found in the packet at the moment of intercepting the packet at the packet processor part, and
- processing the packet according to a set of processing rules that are based on obedience to said certain protocol and take also the original value of the destination information field into account.

52. A method according to claim 51, additionally comprising the steps of:

- receiving from the packet processor part an original value of a certain source information field found in the packet at the moment of intercepting the packet at the packet processor part, and
- processing the packet according to a set of processing rules that are based on obedience to said certain protocol and take also the original value of the source information field into account.

53. A system for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising:

- a packet processor part that is arranged to intercept packets when they are in transit between the untrusted packet-switched information network and the protected domain and to examine the packets in order to determine, whether the packets contain digital data that pertains to a certain protocol,
- an application gateway part and a communications connection between the packet processor part and the application gateway part,
- at the packet processor part, packet processing means that are arranged to process such packets that are not found to contain digital data that would pertain to said certain protocol,
- at the packet processor part, redirecting means that are arranged to redirect to the application gateway part such packets that are found to contain digital data that pertains to said certain protocol, and
- at the application gateway part, application gateway processing means that are arranged to process such packets according to a set of processing rules based on obedience to said certain protocol that are redirected from the packet processor part to the application gateway part; of which the packet processor part is arranged to run as a kernel mode process in a computer device and the application gateway part is arranged to run as a user mode process in a computer device.

54. A system according to claim 53, comprising:

- at the packet processor part, means for replacing an original value of a certain destination information field within a packet with a replacement value that identifies the application gateway part as the destination of the packet,
- means for indicating from the packet processor part to the application gateway part the original value of the destination information field found in the packet at the moment of intercepting the packet at the packet processor part and
- at the application gateway part, means for using the indicated original value of the destination information field at the application gateway part in processing the packet.

55. A system according to claim 54, additionally comprising:

- at the packet processor part, means for replacing an original value of a certain source information field within a packet with a replacement value that identifies the packet processor part as the source of the packet,
- means for indicating from the packet processor part to the application gateway part the original value of the source information field found in the packet at the moment of intercepting the packet at the packet processor part and
- at the application gateway part, means for using the indicated original value of the source information field at the application gateway part in processing the packet.

56. A system according to claim 53, comprising:

- at the packet processor part, means for prepending a header to a packet, the prepended header containing a value that identifies the application gateway part as the destination of the packet,
- at the application gateway part, means for stripping a prepended header from a packet and
- at the application gateway part, means for using the original value of the destination information field in the packet in processing the packet.

57. A system according to claim 56, additionally comprising:

- at the packet processor part, means for inserting into the prepended header also a value that identifies the packet processor part as the source of the packet, and
- at the application gateway part, means for using the original value of the source information field in the packet in processing the packet.

58. A system according to claim 53, comprising a single computer device arranged to run the packet processor part as a kernel mode process and the application gateway part as a user mode process.

59. A system according to claim 53, comprising a first computer device arranged to run the packet processor part as a kernel mode process and a second computer device, separately from said first computer device, arranged to run the application gateway part as a user mode process.

60. A system according to claim 59, wherein the second computer is arranged to run several application gateway parts as simultaneously or alternately active user mode processes.

61. A system according to claim 59, comprising several second computer devices, each of which has a communications connection with the first computer device and each of which is arranged to run at least one application gateway part as a user mode process.

62. A packet processing device for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising:

- packet intercepting means for intercepting packets when they are in transit between the untrusted packet-switched information network and the protected domain,
- packet examining means for examining packets in order to determine, whether they contain digital data that pertains to a certain protocol,
- packet processing means for processing such packets that are not found to contain digital data that would pertain to said certain protocol,
- replacing means for replacing, in packets that are found to contain digital data that pertains to said certain protocol, an original value of a certain destination information field with a replacement value that identifies an application gateway device as the destination of such packets,
- redirecting means for redirecting packets to the application gateway device for processing according to a set of processing rules based on obedience to said certain protocol, and
- signaling means for indicating to the application gateway part the original value of the destination information field found in packets at the moment of intercepting the packets at the packet filtering device.

63. A packet processing device according to claim 62, wherein:

- the replacing means are also adapted to replace, in packets that are found to contain digital data that pertains to said certain protocol, an original value of a certain source information field with a replacement value that identifies the packet processing device as the source of such packets, and
- the signaling means are also adapted to indicate to the application gateway part the original value of the source information field found in packets at the moment of intercepting the packets at the packet filtering device.

64. A packet processing device for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising:

- packet intercepting means for intercepting packets when they are in transit between the untrusted packet-switched information network and the protected domain,
- packet examining means for examining packets in order to determine, whether they contain digital data that pertains to a certain protocol,
- packet processing means for processing such packets that are not found to contain digital data that would pertain to said certain protocol,
- header adding means for prepending, to packets that are found to contain digital data that pertains to said certain protocol, a header containing a value that identifies an application gateway device as the destination of such packets, and
- redirecting means for redirecting packets to the application gateway device for processing according to a set of processing rules based on obedience to said certain protocol.

65. A packet processing device according to claim 64, wherein:

- the header adding means are adapted to insert into the header also a value that identifies the packet processing device as the source of packets that are found to contain digital data that pertains to said certain protocol.

66. An application gateway device for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising:

- means for receiving intercepted and redirected packets from a packet processor device that intercepts packets when they are in transit between the untrusted packet-switched information network and the protected domain,
- means for receiving from the packet processor device an original value of a certain destination information field found in packets at the moment of intercepting the packets at the packet processor part, and
- means for processing packets according to a set of processing rules that are based on obedience to said certain protocol and take also the original value of the destination information fields into account.

67. An application gateway device according to claim 66, additionally comprising means for receiving from the packet processor device an original value of a certain source information field found in packets at the moment of intercepting the packets at the packet processor part, so that the means for processing packets are adapted to process packets according to a set of processing rules that are based on obedience to said certain protocol and take also the original values of the source and destination information fields into account.

68. A software program product for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising:

- a packet processor program that is arranged to intercept packets when they are in transit between the untrusted packet-switched information network and the protected domain and to examine the packets in order to determine, whether the packets contain digital data that pertains to a certain protocol,
- an application gateway program arranged to communicate with the packet processor program,
- at the disposal of the packet processor program, packet processing means that are arranged to process such packets that are not found to contain digital data that would pertain to said certain protocol,

- at the disposal of the packet processor program, redirecting means that are arranged to redirect to the application gateway program such packets that are found to contain digital data that pertains to said certain protocol, and

- at the disposal of the application gateway program, application gateway processing means that are arranged to process such packets according to a set of processing rules based on obedience to said certain protocol that are redirected from the packet processor program to the application gateway program;

of which the packet processor program is arranged to run as a kernel mode process in a computer device and the application gateway program is arranged to run as a user mode process in a computer device.

69. A packet processor software program product for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising:

- packet intercepting means for intercepting packets when they are in transit between the untrusted packet-switched information network and the protected domain,

- packet examining means for examining packets in order to determine, whether they contain digital data that pertains to a certain protocol,

- packet processing means for processing such packets that are not found to contain digital data that would pertain to said certain protocol,

- replacing means for replacing, in packets that are found to contain digital data that pertains to said certain protocol, an original value of a certain destination information field with a replacement value that identifies an application gateway program as the destination of such packets,

- redirecting means for redirecting packets to the application gateway program for processing according to a set of processing rules based on obedience to said certain protocol, and

- signaling means for indicating to the application gateway program the original value of the destination information field found in packets at the moment of intercepting the packets at the packet filter program.

70. A packet processor software program product according to claim 69, wherein:

- the replacing means are also adapted to replace, in packets that are found to contain digital data that pertains to said certain protocol, an original value of a certain source information field with a replacement value that identifies the packet processor program as the source of such packets, and
- the signaling means are also adapted to indicating to the application gateway program the original value of the source information field found in packets at the moment of intercepting the packets at the packet filter program.

71. A packet processor software program product for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising:

- packet intercepting means for intercepting packets when they are in transit between the untrusted packet-switched information network and the protected domain,
- packet examining means for examining packets in order to determine, whether they contain digital data that pertains to a certain protocol,
- packet processing means for processing such packets that are not found to contain digital data that would pertain to said certain protocol,
- header adding means for prepending, to packets that are found to contain digital data that pertains to said certain protocol, a header containing a value that identifies an application gateway program as the destination of such packets, and
- redirecting means for redirecting packets to the application gateway program for processing according to a set of processing rules based on obedience to said certain protocol.

72. A packet processor software program product according to claim 71, wherein the header adding means are adapted to insert, to the header that is prepended to packets that are found to contain digital data that pertains to said certain protocol, a value that identifies the packet processor program as the source of such packets.

73. An application gateway software program product for handling digital data packets at a logical borderline that separates an untrusted packet-switched information network from a protected domain, comprising:

- means for receiving intercepted and redirected packets from a packet processor program that intercepts packets when they are in transit between the untrusted packet-switched information network and the protected domain,
- means for receiving from the packet processor program an original value of a certain destination information field found in packets at the moment of intercepting the packets at the packet processor program, and
- means for processing packets according to a set of processing rules that are based on obedience to said certain protocol and take also the original value of the destination information field into account.

74. An application gateway software program product according to claim 73, additionally comprising means for receiving from the packet processor program an original value of a certain source information field found in packets at the moment of intercepting the packets at the packet processor program, so that the means for processing packets are adapted to process packets according to a set of processing rules that are based on obedience to said certain protocol and take also the original values of the source and destination information fields into account.

X. EVIDENCE APPENDIX - 37 C.F.R. § 41.37(c)(1)(ix)
NONE

XI. RELATED PROCEEDINGS APPENDIX - 37 C.F.R. § 41.37(c)(1)(x)

NONE